Payment Card Industry (PCI)

Payment Application Data Security Standard (PA-DSS)

Guide du programme

Version 1.2

Octobre 2008

Modifications apportées au document

Date	Version	Description
1er octobre 2008	1.2	Aligner le contenu avec la nouvelle procédure PCI DSS v1.2 et implémenter les changements mineurs notés depuis la v1.1 d'origine.

Copyright 2008 PCI Security Standards Council LLC

Table des matières

Modifications apportées au document **1**

Introduction **3**

Publications associées 3
Mises à jour des documents et des exigences de sécurité 3
Terminologie 3
À propos de la PCI 4
Présentation de l'initiative d'alignement PA-DSS 4
Rôles et responsabilités 5

Considérations propres aux fournisseurs – Préparation à la vérification **8**

À quelles applications la norme PA-DSS s'applique-t-elle ? 8
Avant la vérification 9
Documentation et supports nécessaires 9
Calendrier de vérification PA-DSS 10
Évaluateurs de sécurité qualifiés des applications de paiement 10
Services PA-DSS connexes pouvant être proposés par les PA-QSA 10
Support technique lors des tests 11
Accord de diffusion et transmission du rapport 11
Frais 11

Présentation des processus PA-DSS **12**

Figure 1 : Processus d'acceptation des rapports PA-DSS 13
Figure 2 : Changements PA-DSS apportés à des applications listées 14
Figure 3 : Capitalisation et migration d'applications PABP vers la liste PA-DSS 15
Figure 4 : Revalidation annuelle PA-DSS et renouvellement d'applications arrivées à expiration 16
Figure 5 : Programmes d'assurance qualité des PA-QSA pour les vérifications de rapports 17

Présentation du processus d'acceptation des rapports PA-DSS **18**

Modifications apportées aux applications de paiement répertoriées **19**

Renouvellement des applications expirées **22**

Migration et capitalisation d'applications de paiement conformes au programme PABP **23**

Programme d'assurance qualité **25**

Processus d'acceptation des rapports PA-DSS **27**

Notification faisant suite à une faille ou à un incident de sécurité **28**

Clauses et conditions légales **30**

Annexe A : Éléments de la lettre d'acceptation et de la *liste des applications de paiement conformes à la norme PA-DSS* **31**

Annexe B : Identification des builds d'applications de paiement certifiées **34**

Annexe C : Auto-attestation pour les modifications mineures de versions **35**

Copyright 2008 PCI Security Standards Council LLC

Introduction

Publications associées

Les documents suivants constituent la base des évaluations des applications de paiement :

- *Norme de sécurité des données des applications de paiement (PA-DSS) de l'industrie des cartes de paiement (PCI) – Exigences et procédures d'évaluation de sécurité*
- *Norme de sécurité des données des applications de paiement (PA-DSS) de l'industrie des cartes de paiement (PCI) – Procédures de migration*

Les documents complémentaires ci-après sont utilisés conjointement à ceux précédemment cités :

- *Norme de sécurité des données de l'industrie des cartes de paiement (PCI) – Exigences et procédures d'évaluation de sécurité*
- *Norme de sécurité des données de l'industrie des cartes de paiement (PCI) - Glossaire des termes, abréviations et acronymes*
- *Normes de sécurité des données de l'industrie des cartes de paiement (PCI) – Exigences de conformité pour les évaluateurs de sécurité qualifiés (QSA)*
- *Normes de sécurité des données de l'industrie des cartes de paiement (PCI) - Exigences de conformité pour les évaluateurs de sécurité qualifiés – Addendum pour les évaluateurs de sécurité qualifiés des applications de paiement (PA-QSA)*

Remarque :

Les exigences et procédures d'évaluation de sécurité *de la norme PA-DSS listent les exigences techniques spécifiques et fournissent les procédures et le modèle d'évaluation utilisés pour valider la conformité de l'application de paiement et documenter la vérification. Les deux documents sur les exigences de conformité des QSA définissent les exigences auxquelles un PA-QSA doit satisfaire pour pouvoir réaliser des évaluations.*

Tous les documents sont disponibles au format électronique sur le site www.pcisecuritystandards.org.

Mises à jour des documents et des exigences de sécurité

La sécurité est une course sans fin contre les attaquants potentiels. Il est par conséquent nécessaire de régulièrement vérifier, mettre à jour et améliorer les exigences de sécurité utilisées pour l'évaluation des applications de paiement. Le PCI SSC fera en sorte de mettre à jour tous les 24 mois les exigences de sécurité concernant les applications de paiement.

Le PCI SSC se réserve le droit de changer, de modifier ou de retirer des exigences de sécurité à tout moment. En pareille situation, le PCI SSC fera en sorte de travailler en étroite collaboration avec sa communauté d'organisations participantes et de fournisseurs de logiciels, afin de réduire l'impact de telles modifications.

Terminologie

Expressions spécifiques utilisées dans ce document :

- « PCI SSC » désigne le PCI Security Standards Council, LLC (le Conseil des normes de sécurité de la PCI).
- « PABP » (Payment Application Best Practices, meilleures pratiques des applications de paiement) désigne l'ancien programme de Visa, sur lequel est basée la norme PA-DSS (Payment Application Data Security Standard, norme de sécurité des données des applications de paiement).
- « Marques de cartes de paiement » désigne les marques de cartes de paiement qui sont membres du PCI SSC, soit à l'heure actuelle American Express, Discover, JCB, MasterCard et Visa.
- « Applications de paiement » désigne de manière générale toutes les applications de paiement qui stockent, traitent ou transmettent des données de titulaire de carte dans le cadre d'une autorisation ou d'un règlement, lorsque ces applications de paiement sont vendues, distribuées ou cédées sous licence à des parties tierces.

Copyright 2008 PCI Security Standards Council LLC

À propos de la PCI

Le PCI SSC reflète une volonté émanant des acteurs de l'industrie des cartes de paiement (PCI, Payment Card Industry), à tous les niveaux, d'aligner et de normaliser les exigences de sécurité, les procédures d'évaluation de sécurité et les processus d'identification des applications de paiement jugées conformes par un PA-QSA. La norme PA-DSS et les normes associées du PCI SSC définissent un cadre commun pour les évaluations de sécurité, reconnu par toutes les marques de cartes de paiement.

Toutes les parties prenantes du processus de paiement tirent des avantages de l'alignement des exigences :

- les clients vont bénéficier d'une gamme plus étendue d'applications de paiement sécurisées ;
- les clients sont assurés d'utiliser des produits répondant au niveau de conformité requis ;
- les fournisseurs devront simplement réaliser une seule vérification d'application de paiement, qui sera reconnue par toutes les marques de cartes de paiement.

Pour de plus amples informations sur le PCI SSC, reportez-vous au site Web du PCI SSC : www.pcisecuritystandards.org (ci-après dénommé « le site Web »).

Présentation de l'initiative d'alignement PA-DSS

Le présent Guide du programme de la norme PA-DSS de la PCI (Payment Card Industry) illustre un alignement des exigences des marques de cartes de paiement, combinées pour former un ensemble normalisé :

- d'exigences de sécurité et de procédures d'évaluation des applications de paiement ;
- de processus d'identification des applications de paiement jugées conformes par les PA-QSA ;
- de processus permettant la migration vers la liste du PCI SSC des applications de paiement conformes au programme PABP ;
- de processus d'assurance qualité pour les PA-QSA.

Remarque :

Les rapports PA-DSS sont vérifiés et identifiés directement par le PCI SSC.

Il se peut que la conformité conventionnelle aux normes PCI DSS ne s'applique pas directement aux fournisseurs d'applications de paiement car la plupart des fournisseurs ne stockent, ne traitent et ne transmettent pas de données de titulaire de carte. Cependant, étant donné que ces applications de paiement sont utilisées par les clients pour stocker, traiter et transmettre des données de titulaire de carte, et que les clients sont dans l'obligation de respecter les normes PCI DSS, les applications de paiement doivent aider (et non empêcher) le client à se conformer aux normes PCI DSS. Exemples de la façon dont les applications de paiement peuvent empêcher la conformité aux normes PCI DSS :

1. données de bande magnétique stockées sur le réseau du client après expiration du délai d'autorisation ;
2. applications nécessitant que les clients désactivent d'autres fonctions requises par les normes PCI DSS, telles que les programmes antivirus ou les pare-feu, afin que l'application de paiement fonctionne correctement ;
3. utilisation par le fournisseur de méthodes non sécurisées pour se connecter à l'application afin d'apporter une assistance au client.

Les applications de paiement sécurisées, lorsqu'elles sont mises en œuvre dans un environnement conforme PCI DSS, réduisent autant que possible le risque de voir les failles de sécurité compromettre les données de bande magnétique, les codes et valeurs de validation de carte (CAV2, CID, CVC2, CVV2), les codes et les blocs PIN, ainsi que la fraude résultant de ces failles.

Copyright 2008 PCI Security Standards Council LLC

Rôles et responsabilités

Il existe plusieurs parties prenantes au sein de la communauté des applications de paiement. Certaines de ces parties prenantes participent plus directement que d'autres au processus d'évaluation PA-DSS (fournisseurs, QSA et PCI SCC). D'autres, non directement impliquées dans le processus d'évaluation, doivent avoir connaissance du processus global afin de faciliter les décisions professionnelles s'y rapportant.

Les sections suivantes définissent les rôles et responsabilités des parties prenantes dans la communauté des applications de paiement. Les responsabilités associées au processus d'évaluation sont mentionnées pour les parties prenantes impliquées.

Marques de cartes de paiement

American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. sont les marques de cartes de paiement qui ont fondé le PCI SSC. Elles sont responsables du développement et de l'application de tous les programmes relatifs à la conformité avec la norme PA-DSS, y compris des éléments suivants (liste non exhaustive) :

- toute exigence, mandat ou date pour l'utilisation des applications de paiement conformes à la norme PA-DSS ;
- toute amende ou pénalité relative à l'utilisation d'applications de paiement non conformes.

Les marques de cartes de paiement peuvent définir des programmes de conformité, des mandats, des dates, etc., basés sur la norme PA-DSS et les applications de paiement conformes listées par le PCI SSC. Via ces programmes de conformité, les marques de cartes de paiement font la promotion des applications de paiement conformes listées.

Payment Card Industry Security Standards Council (PCI SSC)

Le PCI SSC (Payment Card Industry Security Standards Council, conseil sur les normes de sécurité du secteur des cartes de paiement) est l'organisme de normalisation qui gère les normes du secteur des cartes de paiement, dont les normes PCI DSS et PA-DSS. En ce qui concerne la norme PA-DSS, le PCI SSC :

- constitue un site de stockage centralisé pour les Rapports sur la conformité PA-DSS ;
- réalise des analyses d'assurance qualité sur les Rapports sur la conformité PA-DSS, afin de vérifier la cohérence et la qualité des rapports ;
- dresse sur le site Web la liste des applications de paiement conformes à la norme PA-DSS *(cette liste ne sera pas disponible avant octobre 2008) ;*
- assure la qualification et la formation des PA-QSA pour réaliser des vérifications PA-DSS ;
- gère et met à jour la norme PA-DSS et la documentation connexe selon un processus de gestion du cycle de vie des normes.

Remarque : Le PCI SSC ne valide pas la conformité des rapports. Le rôle des PA-QSA est de documenter la conformité de l'application de paiement à la norme PA-DSS, à la date de l'évaluation. Le PCI SSC réalise en outre une analyse d'assurance qualité afin de garantir une documentation précise et complète par les PA-QSA des évaluations PA-DSS.

Copyright 2008 PCI Security Standards Council LLC

Fournisseurs de logiciels

Les fournisseurs de logiciels (ci-après dénommés « les fournisseurs ») développent les applications de paiement qui stockent, traitent ou transmettent des données de titulaire de carte dans le cadre d'une autorisation ou d'un règlement, puis vendent, distribuent ou cèdent sous licence ces applications de paiement à des parties tierces (clients ou revendeurs/intégrateurs). Responsabilités des fournisseurs :

- Créer des applications de paiement conformes à la norme PA-DSS qui permettent, et n'empêchent pas, la conformité avec les normes PCI DSS de leurs clients. (L'application ne peut pas imposer un paramètre de mise en œuvre ou de configuration enfreignant une exigence des normes PCI DSS.) ;
- respecter les exigences des normes PCI DSS chaque fois que le fournisseur stocke, traite ou transmet des données de titulaire de carte (par exemple, lors du dépannage du client) ;
- créer un *Guide de mise en œuvre de la norme PA-DSS*, spécifique à chaque application, conformément aux exigences de la *Norme de sécurité des données des applications de paiement (PA-DSS)* ;
- former les clients, les revendeurs et les intégrateurs pour l'installation et la configuration des applications de paiement conformément aux normes PCI DSS ;
- s'assurer que les applications de paiement répondent aux exigences de la norme PA-DSS en procédant à une vérification de conformité PA-DSS, conformément aux spécifications des *Exigences et procédures d'évaluation de conformité PCI PA-DSS*.

Les fournisseurs transmettent leurs applications de paiement et la documentation connexe au PA-QSA, pour vérification. Tous les accords et les coûts associés à l'évaluation sont négociés entre le fournisseur et le PA-QSA. Les fournisseurs autorisent leur PA-QSA à transmettre au PCI SSC les rapports de conformité PA-DSS générés.

PA-QSA

Les PA-QSA sont des QSA (Qualified Security Assessors, évaluateurs de sécurité qualifiés) qualifiés et formés par le PCI SSC pour effectuer des vérifications PA-DSS. *Remarque : Tous les QSA ne sont pas des PA-QSA ; un QSA doit répondre à des exigences de qualification supplémentaires pour accéder au statut de PA-QSA.*

Responsabilités des PA-QSA :

- réaliser des évaluations des applications de paiement conformément aux procédures d'évaluation de sécurité et aux exigences de conformité des PA-QSA ;
- formuler un avis sur la conformité de l'application de paiement aux exigences de la norme PA-DSS ;
- fournir dans le Rapport sur la conformité la documentation adéquate permettant de prouver la conformité de l'application de paiement à la norme PA-DSS ;
- transmettre le Rapport sur la conformité au PCI SSC, accompagné de l'attestation de conformité (signée par le PA-QSA et par le fournisseur) ;
- gérer un processus interne d'assurance qualité appliqué à leurs tâches de PA-QSA.

Il appartient aux PA-QSA de spécifier si oui ou non l'application de paiement est conforme. Le PCI SSC ne valide pas les Rapports sur la conformité au niveau de la conformité technique, mais réalise sur ceux-ci des analyses d'assurance qualité, afin de garantir que la preuve de la conformité est correctement documentée dans les rapports.

Copyright 2008 PCI Security Standards Council LLC

Revendeurs et intégrateurs

Les revendeurs et les intégrateurs sont les entités qui vendent, installent et/ou interviennent sur les applications de paiement au nom des fournisseurs de logiciels ou autres. Les revendeurs et intégrateurs assurant des services associés à des applications de paiement conformes à la norme PA-DSS sont chargés de :

- mettre en œuvre uniquement des applications de paiement conformes à la norme PA-DSS dans un environnement conforme aux normes PCI DSS (ou indiquer au commerçant de procéder de la sorte) ;
- configurer ces applications de paiement (lorsque des options de configuration sont fournies) selon le *Guide de mise en œuvre de la norme PA-DSS* remis par le fournisseur *;*
- configurer ces applications de paiement (ou indiquer au commerçant de procéder de la sorte) conformément aux normes PCI DSS ;
- intervenir sur ces applications de paiement (par exemple, dépannage, mises à jour à distance et support distant) conformément au *Guide de mise en œuvre de la norme PA-DSS* et aux normes PCI DSS.

Les revendeurs et les intégrateurs ne soumettent pas les applications de paiement à des évaluations. Seul le fournisseur peut soumettre des produits à une évaluation.

Clients

Les clients sont les commerçants, les fournisseurs de services et autres qui achètent ou reçoivent une application de paiement pour stocker, traiter ou transmettre des données de titulaire de carte dans le cadre de l'autorisation ou du règlement des transactions de paiement. Les clients voulant utiliser des applications conformes à la norme PA-DSS sont chargés de :

Remarque :

Une application de paiement conforme à la norme PA-DSS seule ne garantit pas la conformité avec les normes PCI DSS.

- mettre en œuvre d'une application de paiement selon la norme PA-DSS dans un environnement conforme aux normes PCI DSS ;
- configurer l'application de paiement (lorsque des options de configuration sont fournies) selon le *Guide de mise en œuvre de la norme PA-DSS* remis par le fournisseur ;
- configurer l'application de paiement conformément aux normes PCI DSS ;
- maintenir le statut de conformité aux normes PCI DSS pour la configuration de l'environnement et de l'application de paiement.

Lorsque la liste sera publiée par le PCI SSC, au deuxième semestre 2008, les clients pourront consulter sur le site Web la liste des applications de paiement conformes, ainsi que d'autres supports de référence.

Copyright 2008 PCI Security Standards Council LLC

Considérations propres aux fournisseurs – Préparation à la vérification

À quelles applications la norme PA-DSS s'applique-t-elle ?

Dans le cadre de la norme PA-DSS, une application de paiement se définit comme l'élément qui stocke, traite ou transmet des données de titulaire de carte dans le cadre d'une autorisation ou d'un règlement, lorsque cette application est vendue, distribuée ou cédée sous licence à des parties tierces.

Le guide suivant peut être utilisé pour déterminer si la norme PA-DSS s'applique à une application de paiement donnée :

- La norme PA-DSS s'applique aux applications de paiement généralement vendues « prêtes à l'emploi » sans modification apportée par les fournisseurs de logiciels.
- La norme PA-DSS concerne les applications de paiement fournies dans des modules, habituellement composés d'un module de base et d'autres modules spécifiques aux types de clients ou fonctions, ou personnalisés à la demande du client. Il se peut que la norme PA-DSS s'applique uniquement au module de base si ce module est le seul exécutant les fonctions de paiement (après confirmation par un PA-QSA). Si d'autres modules réalisent des fonctions de paiement, la norme PA-DSS s'applique également à ces modules. Notez que, pour les fournisseurs de logiciels, l'isolement des fonctions de paiement en un seul ou quelques modules de base (en réservant les autres modules pour les fonctions autres que le paiement) constitue une « meilleure pratique ». Cette meilleure pratique (bien qu'elle ne constitue pas une exigence) peut limiter le nombre de modules soumis à la norme PA-DSS.
- La norme PA-DSS NE s'applique PAS à une application de paiement développée pour un seul client et vendue à celui-ci, puisque cette application sera couverte dans le cadre de la vérification de conformité PCI DSS standard du client. Remarque : Une telle application (que l'on peut qualifier d'application « sur mesure ») est vendue à un seul client (en général un commerçant ou un prestataire de services important) et elle est conçue et développée selon les spécifications du client.
- La norme PA-DSS NE s'applique PAS aux applications de paiement développées par des commerçants et des prestataires de services si elles sont utilisées en interne uniquement (et non vendues, distribuées ou cédées sous licence à une partie tierce), puisque de telles applications de paiement doivent être couvertes dans le cadre de la conformité normale du prestataire de services aux normes PCI DSS.

Par exemple, concernant les deux derniers points ci-dessus, le fait que l'application de paiement développée en interne ou sur mesure stocke des données d'authentification sensibles interdites ou autorise des mots de passe complexes doit être couvert dans le cadre de la conformité normale du commerçant ou du prestataire de services aux normes PCI DSS et ne requiert pas d'évaluation PA-DSS distincte.

La liste non exhaustive suivante fournit des exemples d'applications AUTRES que des applications de paiement dans le cadre de la norme PA-DSS (et qui, par conséquent, n'ont pas besoin d'être soumises aux vérifications PA-DSS) :

- les systèmes d'exploitation sur lesquels une application de paiement est installée (par exemple Windows, Unix) ;
- les systèmes de base de données stockant des données de titulaire de carte (par exemple Oracle) ;
- les systèmes de back office stockant les données de titulaire de carte (par exemple, pour les besoins de reporting ou du service client).

Remarque :

Le PCI SSC répertorie UNIQUEMENT les applications de paiement.

Copyright 2008 PCI Security Standards Council LLC

Avant la vérification

- Consultez les exigences des normes PCI DSS et de la norme PA-DSS, ainsi que la documentation connexe, via le site Web.
- Définissez/évaluez l'aptitude de l'application de paiement à se conformer à la norme PA-DSS :
  - réalisez une analyse des écarts entre le mode de fonctionnement de l'application de paiement soumise à la norme PA-DSS et les exigences de cette dernière ;
  - remédiez à tous les écarts potentiels ;
  - le PA-QSA peut, s'il le souhaite, réaliser une pré-évaluation ou une analyse des écarts sur l'application de paiement d'un fournisseur. Si le PA-QSA constate des déficiences empêchant de donner un avis favorable, il remettra au fournisseur de logiciels une liste de fonctions de l'application de paiement devant être optimisées avant que ne débute le processus formel de vérification.
- Définissez si le *Guide de mise en œuvre de la norme PA-DSS* satisfait aux exigences de la norme PA-DSS.

Documentation et supports nécessaires

L'évaluation pose comme exigence que le fournisseur de logiciels transmette au PA-QSA la documentation et les logiciels adéquats.

Tous les documents et informations concernant la norme PA-DSS peuvent être téléchargés via le site Web. Tous les supports associés à l'application de paiement, tels que les CD d'installation, les manuels, le *Guide de mise en œuvre de la norme PA-DSS*, etc., et nécessaires pour la vérification, doivent être transmis à un PA-QSA spécifié sur le site Web et non au PCI SSC. Les informations spécifiques se rapportant à la vérification doivent être demandées directement au PA-QSA.

Exemples de documents et éléments à transmettre au PA-QSA :

1. L'application de paiement avec le manuel de l'opérateur ou les instructions.
2. Les accessoires matériels et logiciels nécessaires pour réaliser des simulations de transactions de paiement.
3. La documentation décrivant toutes les fonctions utilisées pour la saisie et l'émission de données et pouvant être utilisées par des développeurs tiers d'applications. Plus spécifiquement, les fonctions associées aux flux de collecte, d'autorisation de paiement, de règlement et de rejet de débit (lorsqu'ils concernent l'application) doivent être décrites. (Un manuel constitue un exemple de documentation répondant à cette exigence.)
4. La documentation associée à l'installation et à la configuration de l'application, ou qui fournit des informations sur celle-ci. Exemples de telles ressources documentaires :
   - *Guide de mise en œuvre de la norme PA-DSS*
   - Guide d'installation logicielle ou les instructions (selon ce qui est fourni aux clients)
   - Méthode de numérotation des versions appliquée par le fournisseur
   - Documentation sur le contrôle des changements, qui indique la façon dont les changements sont signifiés aux clients
5. Toute documentation complémentaire (schémas et organigrammes, par exemple) contribuant à la vérification de l'application de paiement (le PA-QSA peut, si nécessaire, demander des supports complémentaires).

Copyright 2008 PCI Security Standards Council LLC

Calendrier de vérification PA-DSS

Le temps nécessaire pour une vérification PA-DSS, depuis son lancement jusqu'à sa finalisation, générant une application totalement conforme avec tous ses éléments spécifiés comme « En place », peut varier dans des proportions considérables. Facteurs influant sur la durée nécessaire :

- Degré d'adéquation de l'application à la norme PA-DSS au lancement de la vérification.
  - Les corrections apportées à l'application de paiement en vue de parvenir à la conformité vont faire augmenter le temps nécessaire.
- Degré de finalisation du *Guide de mise en œuvre de la norme PA-DSS* au lancement de la vérification.
  - Les phases de réécriture intensives du *Guide* vont faire augmenter le temps nécessaire.
- Préparation et transmission au PCI SSC par le PA-QSA d'un Rapport sur la conformité PA-DSS de haute qualité.
  - Le temps nécessaire va augmenter si le PCI SSC vérifie le rapport plus d'une fois, en faisant des commentaires au PA-QSA qui doivent à chaque fois être pris en compte.

Tout calendrier de vérification fourni par un PA-QSA doit être considéré comme une estimation, car il peut être basé sur de simples hypothèses selon lesquelles l'application de paiement saura satisfaire rapidement à toutes les exigences de la norme PA-DSS. En cas de problèmes lors des processus de vérification ou d'acceptation, des entretiens entre le PA-QSA, le fournisseur de logiciels et/ou le PCI SSC seront nécessaires. Ces entretiens peuvent influer sur la durée de la vérification et entraîner des retards, et/ou ils peuvent même entraîner l'arrêt prématuré de la vérification (par exemple, si le fournisseur décide de ne pas apporter les changements nécessaires à l'application de paiement pour assurer sa conformité).

Évaluateurs de sécurité qualifiés des applications de paiement

Le PCI SSC assure la qualification et la formation des évaluateurs de sécurité qualifiés des applications de paiement (PA-QSA), pour qu'ils réalisent les évaluations PA-DSS. La liste des PA-QSA est disponible sur le site Web. Ces PA-QSA sont les seuls évaluateurs reconnus par le PCI SSC pour réaliser des évaluations PA-DSS.

Les tarifs et frais facturés par les PA-QSA ne sont pas fixés par le PCI SSC ; ils sont librement négociés entre le PA-QSA et son client. Avant de choisir un PA-QSA, il est recommandé aux entités de s'entretenir avec plusieurs sociétés PA-QSA et de suivre le processus de sélection de fournisseurs de leur entreprise.

Services PA-DSS connexes pouvant être proposés par les PA-QSA

Aucun de ces services n'est exigé ni recommandé par le PCI SSC. Cette liste est fournie afin de donner des exemples des types de services pouvant être proposés par les PA-QSA. Si ces services présentent un intérêt pour votre entreprise, veuillez contacter les PA-QSA pour connaître leur disponibilité et leur prix. Exemples de services PA-DSS connexes :

- Orientation pour la conception d'applications de paiement conformes à la norme PA-DSS.
- Vérification du logiciel d'un fournisseur à sa phase de conception, réponse aux questions par e-mail et téléphone, participation à des téléconférences afin de clarifier les exigences.
- Orientation pour la préparation du *Guide de mise en œuvre de la norme PA-DSS*.
- Services de pré-évaluation (analyse des écarts) avant l'évaluation formelle PA-DSS.
- Orientation pour la mise en conformité de l'application de paiement à la norme PA-DSS, si des écarts ou des non-conformités sont constatés lors de l'évaluation.

Copyright 2008 PCI Security Standards Council LLC

Support technique lors des tests

Il est recommandé au fournisseur de tenir à disposition un employé du support technique qui pourra répondre aux éventuelles questions lors de l'évaluation. Durant la vérification, afin d'accélérer le processus, un contact chez le fournisseur devra être « de garde » afin de débattre des problèmes et de répondre aux questions du PA-QSA.

Accord de diffusion et transmission du rapport

Avant que le PA-QSA ne diffuse le rapport PA-DSS au PCI SSC, le fournisseur doit signer l'*Accord de diffusion fournisseur PA-DSS de l'industrie des cartes de paiement* (ci-après dénommé « l'accord de diffusion »), qui autorise la diffusion du rapport au PCI SSC pour vérification. L'accord de diffusion **doit être transmis directement** au PCI SSC par le PA-QSA, accompagné des rapports PA-DSS.

Frais

Tous les frais associés à l'évaluation PA-DSS faite par le PA-QSA sont négociés entre le PA-QSA et le fournisseur de l'application de paiement ; le fournisseur paye tous les frais directement au PA-QSA.

Les fournisseurs devront s'acquitter de frais d'inscription de 1 250 $ (environ 800 €) pour chaque application de paiement inscrite sur la liste des applications de paiement du PCI SSC.

Dans le cadre du processus de revalidation annuelle (reportez-vous à la section « Revalidation annuelle » dans les pages suivantes de ce document), les frais d'inscription seront facturés par le PCI SSC tous les ans aux fournisseurs de logiciels, pour toutes les applications de paiement appartenant à un fournisseur donné et listées par le PCI SSC à la date de facturation. La date de facturation sera définie sur une base trimestrielle, en fonction du trimestre pendant lequel est intervenue son inscription d'origine. Par exemple, au 1er avril, les fournisseurs de logiciels se verront facturer 1 250 $ par application de paiement listée à la fin du trimestre précédent, le 31 mars. Les fournisseurs ne se verront pas facturer les applications qui sont conformes mais pour lesquelles ils ont choisi de ne pas voir leur produit listé sur le site Web. Remarque : les fournisseurs ne seront pas autorisés à effectuer des manipulations afin de contourner les frais d'inscription. En clair, les fournisseurs ne peuvent pas retirer une application de la liste pour ensuite demander sa réinscription, une fois la date de facturation passée.

Remarque :

Le fournisseur paie tous les frais d'évaluation PA-DSS directement au PA-QSA (ces frais sont négociés entre le fournisseur et le PA-QSA).

Le PCI SSC effectuera une facturation trimestrielle au fournisseur de tous les frais d'inscription, que le fournisseur devra payer directement au PCI SSC.

Copyright 2008 PCI Security Standards Council LLC

Présentation des processus PA-DSS

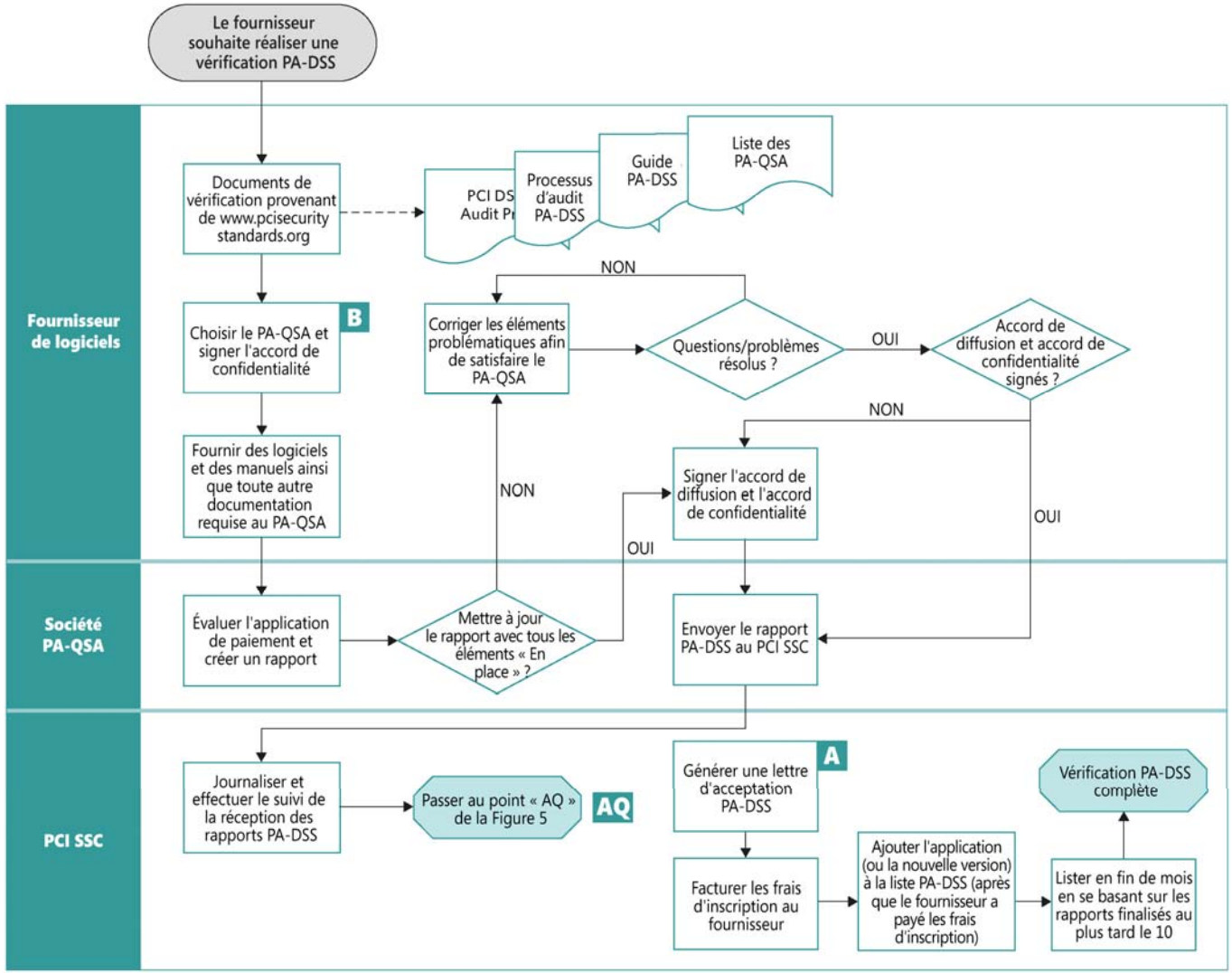
Le processus de vérification PA-DSS est initié par le fournisseur. Le site Web rassemble tous les documents associés qui seront nécessaires au fournisseur pour appliquer le processus de vérification PA-DSS. Le fournisseur sélectionne un PA-QSA dans la liste du PCI SSC, puis négocie les frais et l'accord de confidentialité avec le PA-QSA. Le fournisseur transmet ensuite au PA-QSA le logiciel d'application de paiement, les manuels et toute autre documentation nécessaire. Le PCI SSC va ensuite émettre une lettre d'acceptation (ci-après dénommée « lettre d'acceptation PA-DSS »), confirmant pour chaque application de paiement la bonne réalisation du processus de vérification PA-DSS. Une fois l'application de paiement acceptée, elle est listée sur le site Web.

Les illustrations et descriptions des pages suivantes présentent en détail les composants suivants du programme PA-DSS :

Processus	Illustration	Page n°
Processus d'acceptation des rapports PA-DSS	Figure 1	12
Changements PA-DSS apportés à des applications listées	Figure 2	13
Capitalisation et migration d'applications PABP vers la liste PA-DSS	Figure 3	14
Revalidation annuelle PA-DSS et renouvellement d'applications arrivées à expiration	Figure 4	15
Programmes d'assurance qualité des PA-QSA pour les vérifications de rapports	Figure 5	16

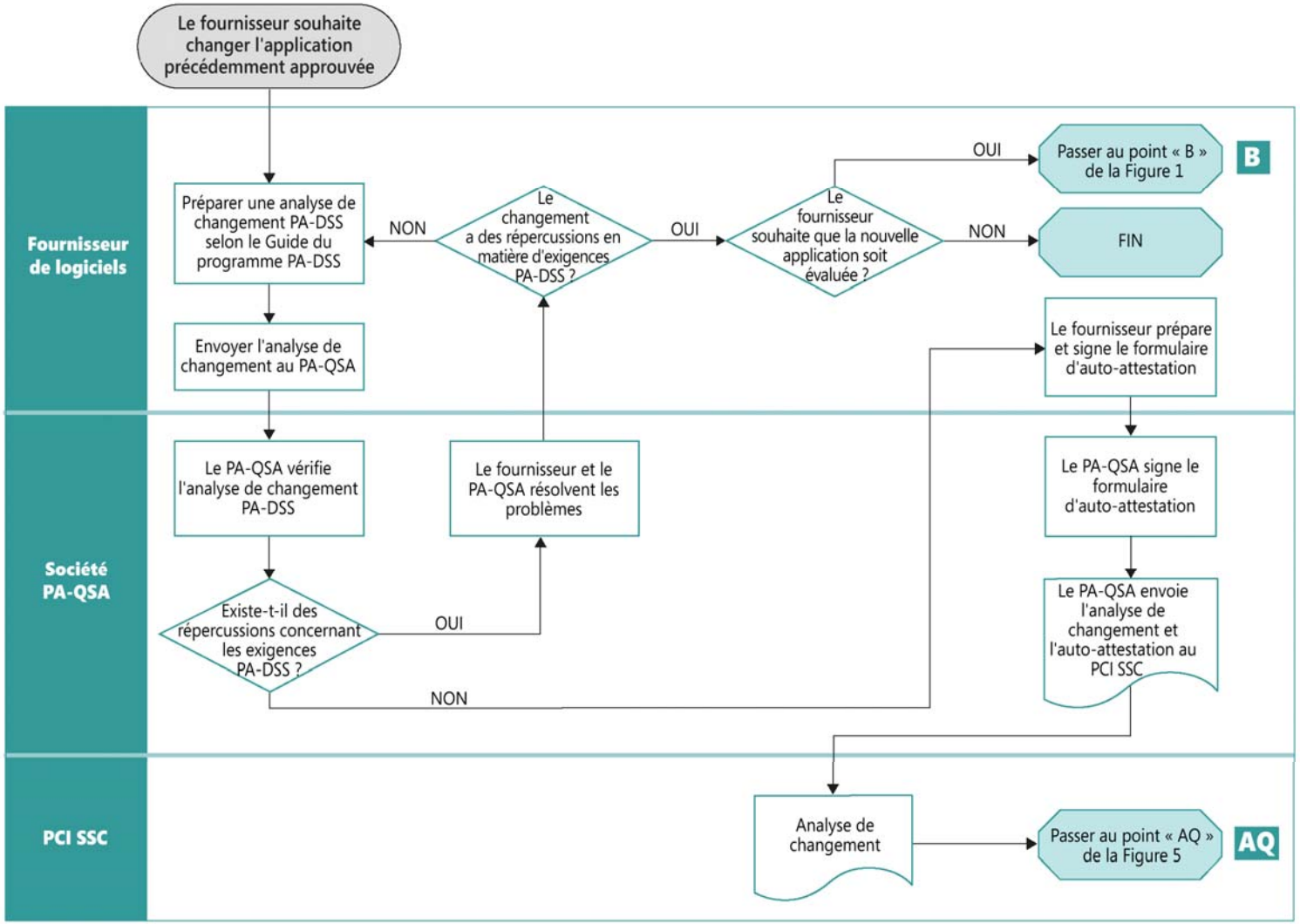
Copyright 2008 PCI Security Standards Council LLC

Figure 1 : Processus d'acceptation des rapports PA-DSS


Le fournisseur souhaite réaliser une vérification PA-DSS
Fournisseur de logiciels
Société PA-QSA
PCI SSC
Documents de vérification provenant de www.pcisecurity standards.org
PCI DS
Audit P
Processus d'audit PA-DSS
Guide PA-DSS
Liste des PA-QSA
Choisir le PA-QSA et signer l'accord de confidentialité
B
Fournir des logiciels et des manuels ainsi que toute autre documentation requise au PA-QSA
Évaluer l'application de paiement et créer un rapport
Journaliser et effectuer le suivi de la réception des rapports PA-DSS
Passer au point « AQ » de la Figure 5
AQ
Corriger les éléments problématiques afin de satisfaire le PA-QSA
NON
Questions/problèmes résolus ?
OUI
Accord de diffusion et accord de confidentialité signés ?
NON
OUI
Signer l'accord de diffusion et l'accord de confidentialité
Mettre à jour le rapport avec tous les éléments « En place » ?
NON
OUI
Envoyer le rapport PA-DSS au PCI SSC
Générer une lettre d'acceptation PA-DSS
A
Facturer les frais d'inscription au fournisseur
Ajouter l'application (ou la nouvelle version) à la liste PA-DSS (après que le fournisseur a payé les frais d'inscription)
Lister en fin de mois en se basant sur les rapports finalisés au plus tard le 10
Vérification PA-DSS complète

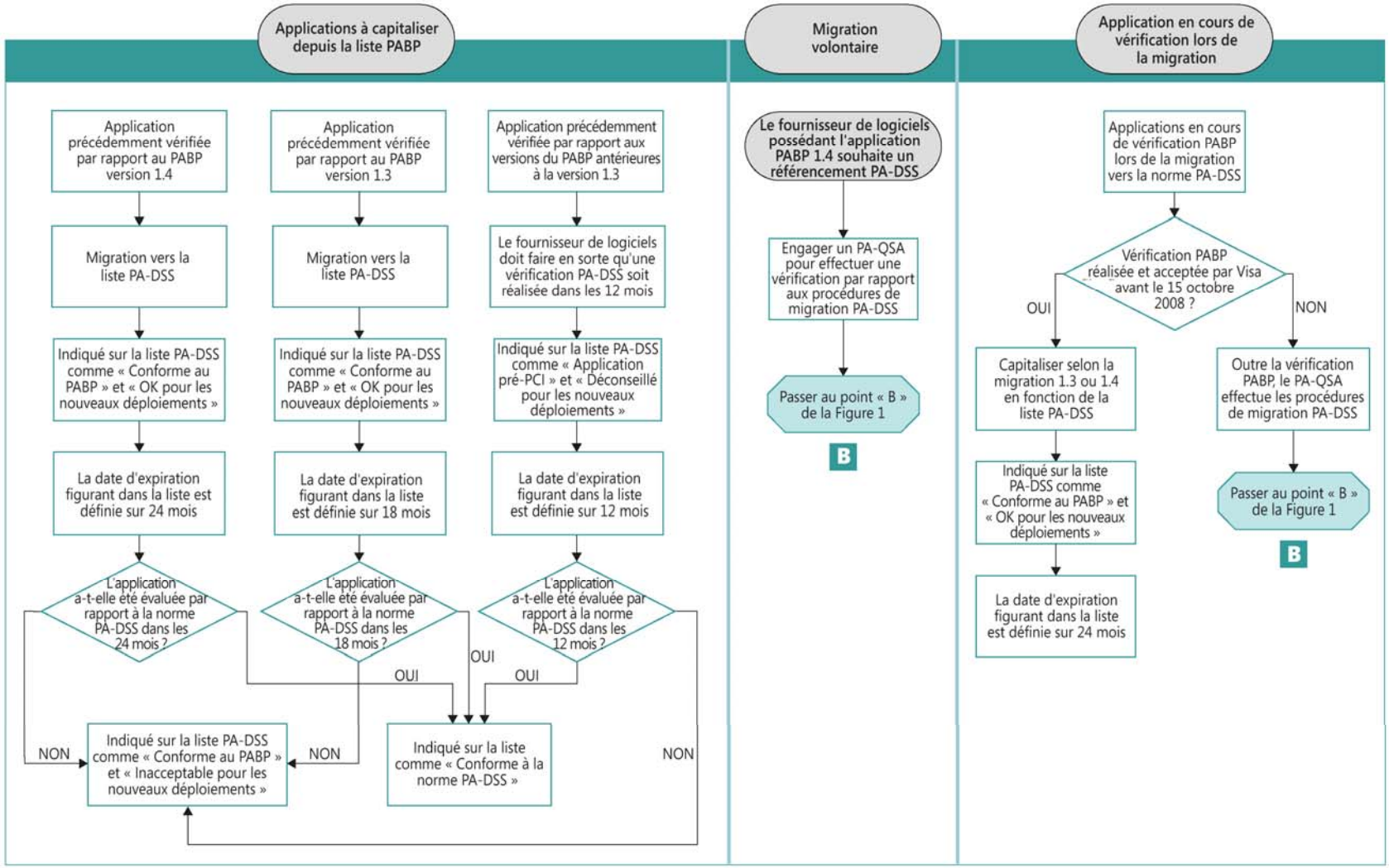
Copyright 2008 PCI Security Standards Council LLC

Figure 2 : Changements PA-DSS apportés à des applications listées


Le fournisseur souhaite changer l'application précédemment approuvée
Fournisseur de logiciels
Préparer une analyse de changement PA-DSS selon le Guide du programme PA-DSS
Envoyer l'analyse de changement au PA-QSA
NON
Le changement a des répercussions en matière d'exigences PA-DSS ?
OUI
Le fournisseur souhaite que la nouvelle application soit évaluée ?
OUI
Passer au point « B » de la Figure 1
B
NON
FIN
Le fournisseur prépare et signe le formulaire d'auto-attestation
Société PA-QSA
Le PA-QSA vérifie l'analyse de changement PA-DSS
Le fournisseur et le PA-QSA résolvent les problèmes
Existe-t-il des répercussions concernant les exigences PA-DSS ?
OUI
NON
Le PA-QSA signe le formulaire d'auto-attestation
Le PA-QSA envoie l'analyse de changement et l'auto-attestation au PCI SSC
PCI SSC
Analyse de changement
Passer au point « AQ » de la Figure 5
AQ

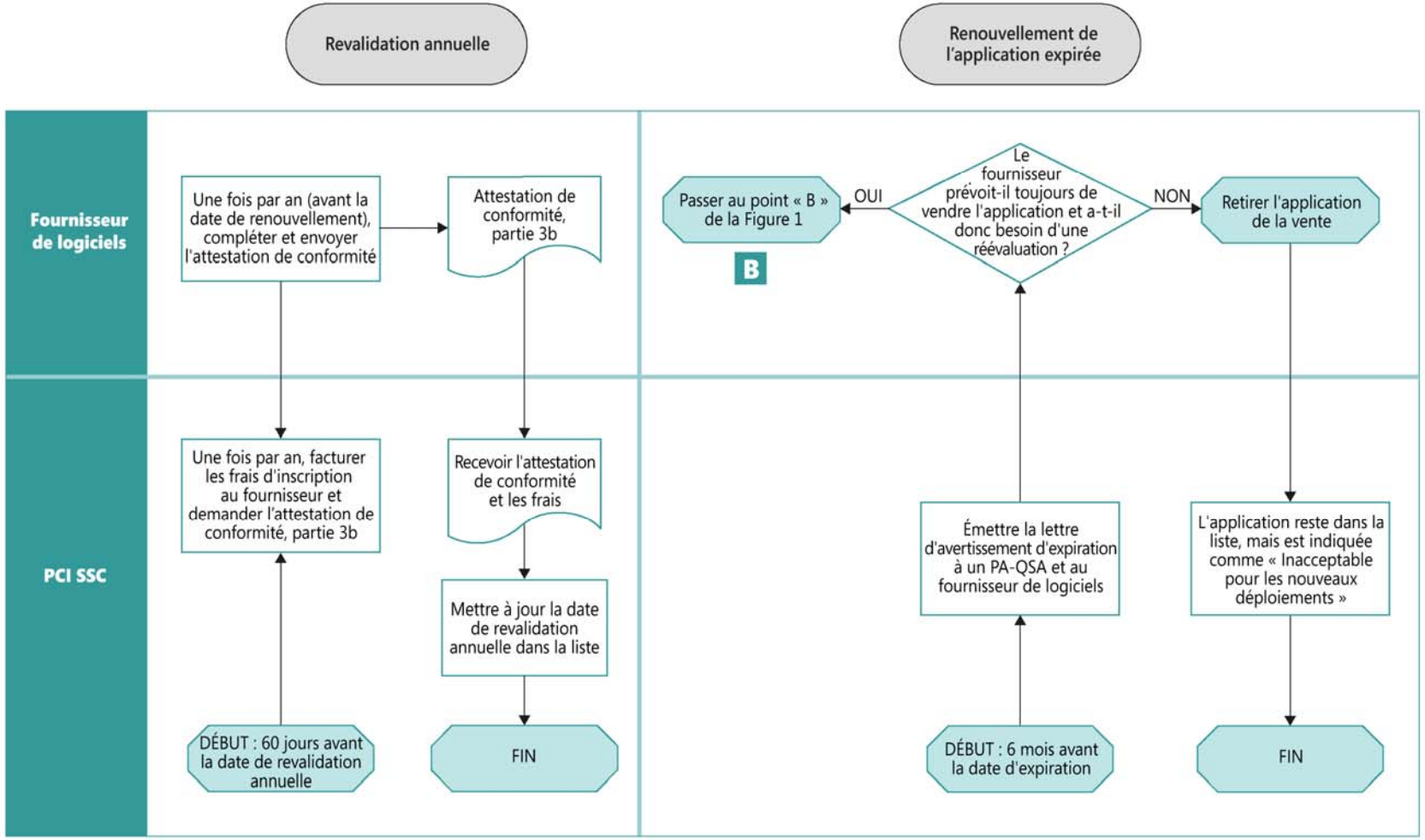
Copyright 2008 PCI Security Standards Council LLC

Figure 3 : Capitalisation et migration d'applications PABP vers la liste PA-DSS


Applications à capitaliser depuis la liste PABP
Migration volontaire
Application en cours de vérification lors de la migration
Application précédemment vérifiée par rapport au PABP version 1.4
Application précédemment vérifiée par rapport au PABP version 1.3
Application précédemment vérifiée par rapport aux versions du PABP antérieures à la version 1.3
Migration vers la liste PA-DSS
Migration vers la liste PA-DSS
Le fournisseur de logiciels doit faire en sorte qu'une vérification PA-DSS soit réalisée dans les 12 mois
Indiqué sur la liste PA-DSS comme « Conforme au PABP » et « OK pour les nouveaux déploiements »
Indiqué sur la liste PA-DSS comme « Conforme au PABP » et « OK pour les nouveaux déploiements »
Indiqué sur la liste PA-DSS comme « Application pré-PCI » et « Déconseillé pour les nouveaux déploiements »
La date d'expiration figurant dans la liste est définie sur 24 mois
La date d'expiration figurant dans la liste est définie sur 18 mois
La date d'expiration figurant dans la liste est définie sur 12 mois
L'application a-t-elle été évaluée par rapport à la norme PA-DSS dans les 24 mois ?
L'application a-t-elle été évaluée par rapport à la norme PA-DSS dans les 18 mois ?
L'application a-t-elle été évaluée par rapport à la norme PA-DSS dans les 12 mois ?
OUI
OUI
OUI
NON
NON
NON
Indiqué sur la liste PA-DSS comme « Conforme au PABP » et « Inacceptable pour les nouveaux déploiements »
Indiqué sur la liste comme « Conforme à la norme PA-DSS »
Le fournisseur de logiciels possédant l'application PABP 1.4 souhaite un référencement PA-DSS
Engager un PA-QSA pour effectuer une vérification par rapport aux procédures de migration PA-DSS
Passer au point « B » de la Figure 1
B
Applications en cours de vérification PABP lors de la migration vers la norme PA-DSS
Vérification PABP réalisée et acceptée par Visa avant le 15 octobre 2008 ?
OUI
NON
Capitaliser selon la migration 1.3 ou 1.4 en fonction de la liste PA-DSS
Outre la vérification PABP, le PA-QSA effectue les procédures de migration PA-DSS
Indiqué sur la liste PA-DSS comme « Conforme au PABP » et « OK pour les nouveaux déploiements »
Passer au point « B » de la Figure 1
B
La date d'expiration figurant dans la liste est définie sur 24 mois

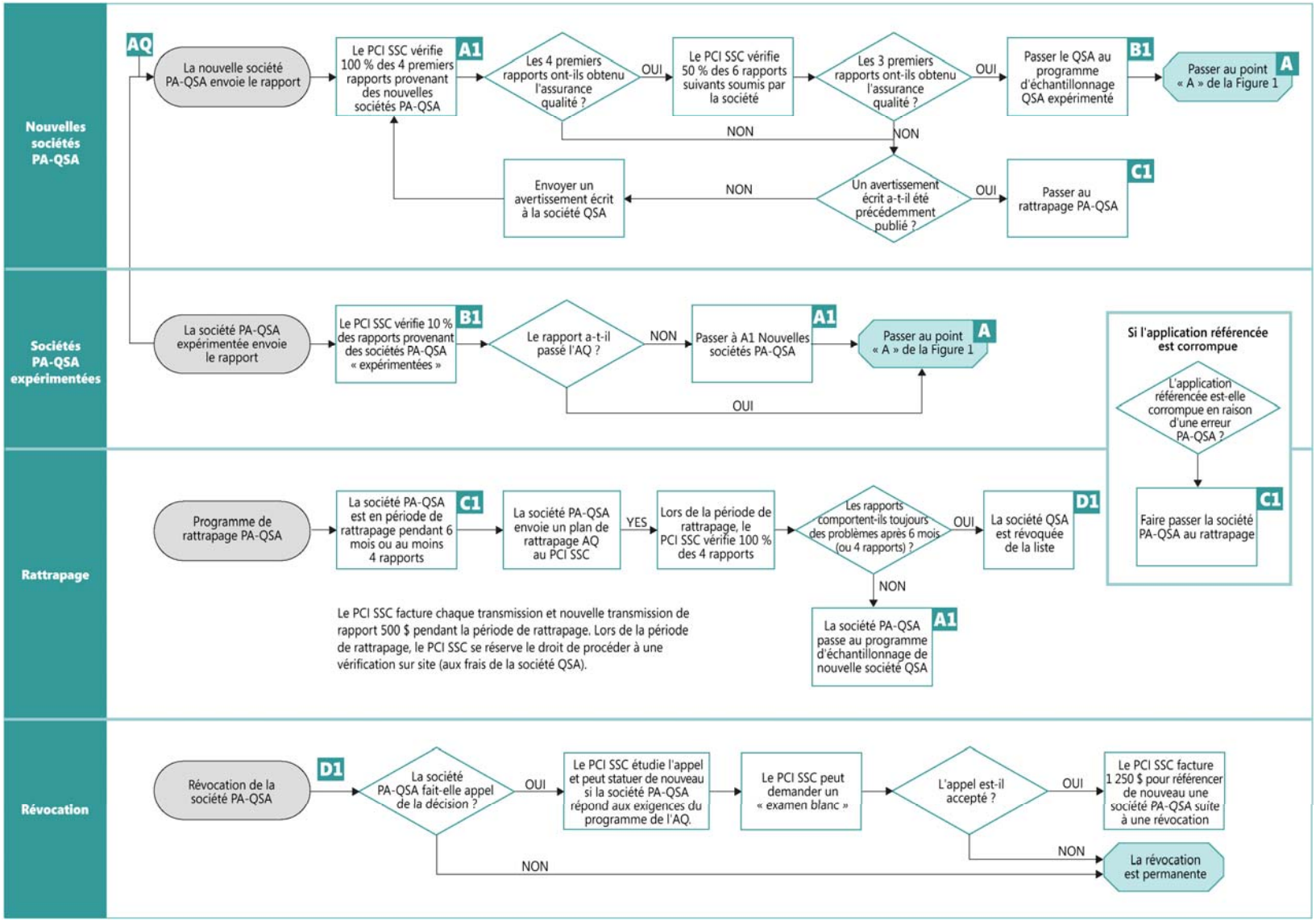
Copyright 2008 PCI Security Standards Council LLC

Figure 4 : Revalidation annuelle PA-DSS et renouvellement d'applications arrivées à expiration


Revalidation annuelle
Renouvellement de l'application expirée
Fournisseur de logiciels
PCI SSC
Une fois par an (avant la date de renouvellement), compléter et envoyer l'attestation de conformité
Attestation de conformité, partie 3b
Passer au point « B » de la Figure 1
B
OUI
Le fournisseur prévoit-il toujours de vendre l'application et a-t-il donc besoin d'une réévaluation ?
NON
Retirer l'application de la vente
Une fois par an, facturer les frais d'inscription au fournisseur et demander l'attestation de conformité, partie 3b
Recevoir l'attestation de conformité et les frais
Mettre à jour la date de revalidation annuelle dans la liste
Émettre la lettre d'avertissement d'expiration à un PA-QSA et au fournisseur de logiciels
L'application reste dans la liste, mais est indiquée comme « Inacceptable pour les nouveaux déploiements »
DÉBUT : 60 jours avant la date de revalidation annuelle
FIN
DÉBUT : 6 mois avant la date d'expiration
FIN

Copyright 2008 PCI Security Standards Council LLC

Figure 5 : Programmes d'assurance qualité des PA-QSA pour les vérifications de rapports


Nouvelles sociétés PA-QSA
AQ
La nouvelle société PA-QSA envoie le rapport
Le PCI SSC vérifie 100 % des 4 premiers rapports provenant des nouvelles sociétés PA-QSA
A1
Les 4 premiers rapports ont-ils obtenu l'assurance qualité ?
OUI
Le PCI SSC vérifie 50 % des 6 rapports suivants soumis par la société
Les 3 premiers rapports ont-ils obtenu l'assurance qualité ?
OUI
Passer le QSA au programme d'échantillonnage QSA expérimenté
B1
Passer au point « A » de la Figure 1
A
NON
NON
Envoyer un avertissement écrit à la société QSA
NON
Un avertissement écrit a-t-il été précédemment publié ?
OUI
Passer au rattrapage PA-QSA
C1
Sociétés PA-QSA expérimentées
La société PA-QSA expérimentée envoie le rapport
Le PCI SSC vérifie 10 % des rapports provenant des sociétés PA-QSA « expérimentées »
B1
Le rapport a-t-il passé l'AQ ?
NON
Passer à A1 Nouvelles sociétés PA-QSA
A1
Passer au point « A » de la Figure 1
A
OUI
Si l'application référencée est corrompue
L'application référencée est-elle corrompue en raison d'une erreur PA-QSA ?
Faire passer la société PA-QSA au rattrapage
C1
Rattrapage
Programme de rattrapage PA-QSA
La société PA-QSA est en période de rattrapage pendant 6 mois ou au moins 4 rapports
C1
La société PA-QSA envoie un plan de rattrapage AQ au PCI SSC
YES
Lors de la période de rattrapage, le PCI SSC vérifie 100 % des 4 rapports
Les rapports comportent-ils toujours des problèmes après 6 mois (ou 4 rapports) ?
OUI
La société QSA est révoquée de la liste
D1
NON
La société PA-QSA passe au programme d'échantillonnage de nouvelle société QSA
A1
Le PCI SSC facture chaque transmission et nouvelle transmission de rapport 500 $ pendant la période de rattrapage. Lors de la période de rattrapage, le PCI SSC se réserve le droit de procéder à une vérification sur site (aux frais de la société QSA).
Révocation
Révocation de la société PA-QSA
D1
La société PA-QSA fait-elle appel de la décision ?
OUI
Le PCI SSC étudie l'appel et peut statuer de nouveau si la société PA-QSA répond aux exigences du programme de l'AQ.
Le PCI SSC peut demander un « examen blanc »
L'appel est-il accepté ?
OUI
Le PCI SSC facture 1 250 $ pour référencer de nouveau une société PA-QSA suite à une révocation
NON
NON
La révocation est permanente

Copyright 2008 PCI Security Standards Council LLC

Présentation du processus d'acceptation des rapports PA-DSS

Notez que tous les rapports PA-DSS et autres supports soumis au PCI SSC doivent être rédigés en anglais.

Le PA-QSA vérifie l'application de paiement conformément aux *Procédures d'évaluation de sécurité PA-DSS* et rédige un rapport avec le fournisseur. Si tous les points abordés dans le rapport sont « en place », le fournisseur signe l'*Accord de diffusion,* que le PA-QSA envoie ensuite au PCI SSC. Si certains points abordés dans le rapport ne sont pas « en place », le fournisseur doit mettre en évidence les points en question dans le rapport. Il peut s'agir par exemple d'une mise à jour logicielle ou d'une mise à jour de la documentation destinée aux utilisateurs. Lorsque le PA-QSA estime que tous les problèmes ont été résolus par le fournisseur, ce dernier signe l'*Accord de diffusion* que le PA-QSA envoie ensuite au PCI SSC.

Le PCI SSC reçoit le rapport et effectue une dernière vérification d'assurance qualité. Si le rapport répond aux exigences d'assurance qualité, conformément aux exigences de conformité pour les évaluateurs de sécurité qualifiés et aux documents connexes, le PCI SSC envoie une lettre d'acceptation PA-DSS au fournisseur et ajoute l'application à la liste du PCI SSC avant la fin du mois, pour les applications qui ont été finalisées avant le 10 du mois. Si le PCI SSC remarque des problèmes de qualité au niveau du rapport, il les communique au PA-QSA. Dès lors, il incombe au PA-QSA de résoudre ces problèmes avec le PCI SSC. La résolution des problèmes peut se limiter à la mise à jour du rapport avec la documentation appropriée, de manière à obtenir un rapport conforme aux décisions du PA-QSA. Toutefois, si les problèmes en question entraînent un examen plus approfondi, le PA-QSA doit spécifier au fournisseur qu'un test supplémentaire est nécessaire et le programmer avec lui.

Le schéma du processus d'acceptation des rapports est détaillé dans la Figure 1.

Copyright 2008 PCI Security Standards Council LLC

Modifications apportées aux applications de paiement répertoriées

Les fournisseurs peuvent mettre à jour les applications de paiement précédemment répertoriées pour différentes raisons, pour ajouter une fonctionnalité auxiliaire ou mettre à niveau la base de référence ou l'application principale par exemple.

Au niveau de la norme PA-DSS, on rencontre généralement trois types de scénarios :

1. Les changements mineurs apportés à une application de paiement répertoriée n'ont pas d'impact sur les exigences PA-DSS. Dans ce cas, le fournisseur de logiciels documente les modifications de la nouvelle version à répertorier en vue de la vérification du PA-QSA. Pour plus d'informations, reportez-vous à la section *Aucun impact sur les exigences PA-DSS*.
2. Les modifications apportées à une application de paiement répertoriée ont un impact potentiel sur les exigences PA-DSS. Dans ce cas, le fournisseur de logiciels soumet la nouvelle version de l'application de paiement à répertorier, en vue de la vérification complète à effectuer par le PA-QSA. Pour plus d'informations, reportez-vous à la section *Impact potentiel sur les exigences PA-DSS*.
3. Aucune modification apportée à une application de paiement répertoriée. Dans ce cas, seul un formulaire d'attestation annuel est requis. Pour plus d'informations, reportez-vous à la section *Aucune modification apportée à l'application de paiement répertoriée*.

Si le fournisseur met à jour des applications précédemment répertoriées et s'il souhaite que la notification de mise à jour de l'application de paiement figure sur la liste, il doit soumettre les détails des modifications au PA-QSA, de préférence à celui qui a effectué la première vérification.

Par la suite, le PA-QSA détermine si une réévaluation de l'application de paiement est nécessaire. Cette décision peut dépendre de l'impact éventuel des modifications sur la sécurité de l'application. Elle peut également être encouragée par la portée ou l'importance des modifications apportées. Il est en effet possible que la modification n'affecte qu'une fonctionnalité auxiliaire et ne se répercute pas sur l'application de paiement principale.

Si une application de paiement répertoriée a subi des modifications susceptibles d'affecter les exigences PA-DSS, et/ou si le fournisseur souhaite que ces informations figurent dans la *lettre d'acceptation PA-DSS* et sur le site Web révisé, il doit fournir au PA-QSA une documentation appropriée spécifiant les modifications afin que celui-ci détermine si une évaluation complète est nécessaire. Si le PA-QSA convient avec le fournisseur de logiciels que les modifications documentées n'ont pas d'impact sur les exigences PA-DSS, ce dernier prépare et signe un formulaire d'auto-attestation de modification, que le PA-QSA signe également et transmet ensuite au PCI SSC. Le PCI SSC intègre alors les mises à jour à la *lettre d'acceptation PA-DSS* révisée et sur le site Web. Pour plus d'informations, reportez-vous à la section ci-dessous *Aucun impact sur les exigences PA-DSS : Nouvelle vérification PA-DSS non requise*.

Remarque :

Si les fournisseurs d'applications de paiement pouvaient moduler la fonctionnalité de paiement, cela permettrait de diminuer le nombre de réévaluations dues aux modifications qui n'ont pas d'impact sur la fonctionnalité de paiement et sur sa sécurité.

Le schéma du processus de modification des applications répertoriées est détaillé dans la Figure 2.

Copyright 2008 PCI Security Standards Council LLC

Aucun impact sur les exigences PA-DSS : Nouvelle vérification PA-DSS non requise

Si une application de paiement précédemment répertoriée est révisée et si la révision révèle une modification mineure n'affectant pas sa sécurité, une documentation sur les modifications (une « analyse de changement ») peut être soumise au PA-QSA pour vérification. Il est fortement recommandé au fournisseur de faire appel au PA-QSA qui a effectué la première évaluation.

L'analyse de changement soumise par le fournisseur de logiciels au PA-QSA doit au minimum contenir les informations suivantes :

- le nom de l'application de paiement ;
- le numéro de version de l'application de paiement ;
- le nom et le numéro de version de l'application de paiement associée figurant actuellement sur la liste du PCI SSC ;
- la description de la modification apportée ;
- les raisons de la modification ;
- l'impact éventuel sur les données de titulaire de carte et les fonctions de paiement, ainsi que la nature de l'impact ;
- la description du fonctionnement du processus de modification ;
- la description du test réalisé par le fournisseur pour valider l'absence d'impact sur les exigences de sécurité PA-DSS ;
- les éléments qui expliquent comment et pourquoi les exigences PA-DSS ne sont pas affectées ;
- La description de l'intégration de cette modification dans la méthodologie de gestion des versions appliquée par le fournisseur, incluant la façon dont ce numéro de version indique que la modification est « mineure » ;
- le cas échéant, la description des pratiques/modules de programmation et la démonstration que ces pratiques n'ont pas d'incidences négatives sur les exigences.

Si le PA-QSA convient que la modification, telle que documentée dans l'analyse de changement du fournisseur, n'a pas d'impact négatif sur la sécurité de l'application de paiement, (i) il le spécifie au fournisseur de logiciels, (ii) celui-ci prépare et signe une auto-attestation de modification et l'envoie au PA-QSA, (iii) le PA-QSA la signe également et la transmet, accompagnée de l'analyse de changement, au PCI SSC, qui (iv) vérifie le formulaire et la documentation dans une optique d'assurance qualité.

Si le PCI SSC estime que la modification n'affecte pas les exigences PA-DSS :

- une lettre d'acception PA-DSS révisée est envoyée au fournisseur ;
- la liste des applications de paiement conformes à la norme PA-DSS du site Web est mise à jour ;
- la date d'expiration et le numéro de version de l'application répertoriée seront les mêmes que ceux de l'application de paiement « parente».

Si le PCI SSC constate des problèmes de qualité relatifs à l'auto-attestation de modification, il les communique au PA-QSA. Les problèmes sont ensuite traités conformément à la procédure décrite précédemment.

Impact potentiel sur les exigences PA-DSS : Nouvelle vérification PA-DSS requise

Si les modifications apportées à l'application de paiement ont un impact sur les exigences PA-DSS, l'application de paiement doit de nouveau être soumise à une évaluation PA-DSS. Le PA-QSA soumet alors un nouveau rapport PA-DSS au PCI SSC pour acceptation. Dans ce cas, le fournisseur peut d'abord soumettre la documentation de modification au PA-QSA, qui détermine ensuite si cette dernière affecte la sécurité de l'application de paiement, conformément aux exigences PA-DSS en vigueur.

Copyright 2008 PCI Security Standards Council LLC

Aucune modification apportée à l'application de paiement répertoriée : Revalidation annuelle requise

Chaque année, à la date de revalidation indiquée sur la liste, le fournisseur de logiciels doit soumettre un formulaire d'attestation de conformité en remplissant la partie 3b. Le formulaire d'attestation de conformité est disponible dans l'annexe C de la norme PA-DSS.

Le schéma du processus de revalidation annuelle est détaillé dans la Figure 4.

Copyright 2008 PCI Security Standards Council LLC

Renouvellement des applications expirées

Lorsqu'une application arrive à expiration, le PCI SSC en avertit le fournisseur de logiciels. Le fournisseur dispose alors de deux options :

1. Le fournisseur souhaite continuer à vendre l'application. Dans ce cas, il contacte un PA-QSA et soumet son application de paiement à une réévaluation.
2. Le fournisseur ne vend plus l'application. Dans ce cas, le PCI SSC définit l'application de paiement répertoriée au statut « Inacceptable pour les nouveaux déploiements » après la date d'expiration.

Notez que si le fournisseur choisit de continuer à vendre l'application, celle-ci conserve son statut « Acceptable pour les nouveaux déploiements » sur la liste du PCI SSC une fois revalidée par le processus d'évaluation PA-DSS et une nouvelle date d'expiration est définie.

Le schéma du processus de renouvellement des applications expirées est détaillé dans la Figure 4.

Copyright 2008 PCI Security Standards Council LLC

Migration et capitalisation d'applications de paiement conformes au programme PABP

Capitalisation d'applications PABP sur la liste PABP d'ici le 15 octobre 2008

Le PCI SSC capitalise (transfère) les applications conformes au programme PABP existantes sur la liste du PCI SSC. Cette approche de capitalisation permet aux applications précédemment évaluées et jugées conformes au programme PABP de continuer à être déployées jusqu'à ce que de nouvelles applications de paiement conformes à la norme PA-DSS soient disponibles.

Une approche évolutive a été appliquée aux dates d'expiration des applications PABP, en fonction de la version des exigences utilisées pour les évaluer. Afin de rester sur la liste PCI SSC sous le statut « Acceptable pour les nouveaux déploiements », les applications conformes au programme PABP doivent être évaluées selon la norme PA-DSS et le calendrier prescrit. Si une application conforme au programme PABP n'est pas évaluée selon la norme PA-DSS et le calendrier prescrit, l'application figurera sur la liste du PCI SSC, mais sous le statut « Inacceptable pour les nouveaux déploiements ».

Remarque :

La liste du PCI SSC fait la distinction entre les « nouveaux déploiements » et les « déploiements existants ». De manière générale, la durée de vie des applications de paiement une fois déployées est longue, allant parfois jusqu'à 10 ou 15 ans. Le PCI SSC a conscience que la procédure de déploiement des applications de paiement peut être complexe et coûteuse, et que la mise à jour annuelle des applications de paiement par les commerçants et les acquéreurs n'est guère pratique.

Le tableau suivant indique les dates d'expiration respectives et les notes qui seront incluses dans la *liste des applications de paiement conformes à la norme PA-DSS* pour les versions du programme PABP, ainsi que pour les vérifications PA-DSS, conformément à la version 1.1 de la norme PA-DSS en vigueur.

Version	Date d'expiration	Liste du PCI SSC avant expiration		Liste du PCI SSC après expiration	
		Notes de conformité	Notes de déploiement	Notes de conformité	Notes de déploiement
PABP 1.4	24 mois	Conforme au programme PABP	Acceptable pour les nouveaux déploiements	Conforme au programme PABP	Inacceptable pour les nouveaux déploiements
PABP 1.3	18 mois	Conforme au programme PABP	Acceptable pour les nouveaux déploiements	Conforme au programme PABP	Inacceptable pour les nouveaux déploiements
Avant le programme PABP 1.3	12 mois	Application pré-PCI	Déconseillé pour les nouveaux déploiements	Application pré-PCI	Inacceptable pour les nouveaux déploiements
PA-DSS 1.1	3 ans après la modification de la norme	Conforme à la norme PA-DSS	Acceptable pour les nouveaux déploiements	Conforme à la norme PA-DSS	Inacceptable pour les nouveaux déploiements

Le schéma du processus de capitalisation et de migration d'applications PABP est détaillé dans la Figure 3.

Applications en cours de vérification PABP lors de la migration

Un délai de tolérance d'environ six mois a débuté à compter de la sortie de la norme PA-DSS version 1.1, permettant aux PA-QSA de se familiariser avec la nouvelle norme, de suivre une formation et de se qualifier pour réaliser des vérifications PA-DSS. De la même façon, les fournisseurs ont pu utiliser cette période pour se familiariser avec la norme PA-DSS et appliquer les nouvelles exigences PA-DSS lors du développement de leurs nouvelles applications de paiement.

Copyright 2008 PCI Security Standards Council LLC

Pendant la période de tolérance, les applications peuvent continuer à être évaluées par rapport au programme PABP version 1.4. La période de tolérance s'étend jusqu'au **15 octobre 2008**. Les rapports soumis au-delà de cette date ne seront pas acceptés et n'obtiendront pas l'attestation de conformité au programme PABP.[1]

Les rapports basés sur le programme PABP version 1.4 et soumis après le 15 octobre 2008 doivent être soumis aux *procédures de migration PA-DSS*. Le PA-QSA peut utiliser les résultats du rapport PABP, mais doit également joindre une réévaluation lors de l'envoi au PCI SSC, conformément aux *procédures de migration PA-DSS*.

Le fournisseur peut également choisir de faire évaluer son application de paiement conformément à la norme PA-DSS à tout moment après la sortie de la nouvelle norme.

Procédures de migration PA-DSS

Les procédures de migration PA-DSS doivent être utilisées par les évaluateurs de sécurité qualifiés des applications de paiement (PA-QSA), le cas échéant, pour assurer la migration d'une application depuis la liste Visa des applications de paiement conformes au programme PABP[2] vers la liste du PCI SSC des applications de paiement conformes à la norme PA-DSS[3].

Remarque : Le PCI SSC assure la capitalisation (ou le transfert) des applications de paiement conformes au programme PABP versions 1.3 et 1.4 vers la liste des applications de paiement conformes à la norme PA-DSS, pour une durée respective de 18 et 24 mois. Passé ce délai, une vérification PA-DSS est exigée.

Ces procédures de migration sont applicables dans les scénarios suivants :

Application obligatoire des procédures de migration : Si une application de paiement est soumise à une vérification PABP qui n'est pas terminée ni validée par Visa avant le 15.10.08, alors l'application de ces procédures de migration est ***obligatoire*** pour que le PCI SSC reconnaisse ces applications comme conformes à la norme PA-DSS. **Les vérifications faites uniquement selon le programme PABP NE seront PLUS acceptées après le 15.10.08**.

Remarque :

La même société PA-QSA que celle contactée pour réaliser la vérification PABP doit être sollicitée pour appliquer les procédures de migration PA-DSS.

Application volontaire des procédures de migration : Conformément à la *Remarque* ci-dessus, si un fournisseur d'applications de paiement dispose d'applications éligibles à une capitalisation, mais qu'il souhaite qu'une application conforme au programme PABP version 1.3 ou 1.4 soit répertoriée comme « Conforme à la norme PA-DSS », alors ces procédures de migration doivent être appliquées. Un PA-QSA appliquera les procédures et transmettra le rapport conformément au Guide du programme PA-DSS, afin que le PCI SSC reconnaisse les applications validées selon le programme PABP versions 1.3 et 1.4.

Pour plus d'informations sur les procédures de migration PA-DSS, reportez-vous à la section *Procédures de migration PA-DSS du programme PABP* du site Web.

---

[1] Si l'application de paiement est évaluée par rapport au programme PABP version 1.4 et soumise avant le 15 octobre 2008, et si le rapport présente des problèmes de qualité, la situation fera l'objet d'une exception. Cette application peut poursuivre sa vérification conformément au programme PABP version 1.4 jusqu'à la résolution des problèmes de qualité. Les exceptions de ce type seront autorisées jusqu'au 15 avril 2009.

[2] Vérification par rapport au programme PABP (Payment Application Best Practices, meilleurs pratiques des applications de paiement), version 1.3 ou 1.4

[3] Vérification par rapport à la norme PA-DSS (Payment Application Data Security Standard, norme de sécurité des données des applications de paiement), version 1.1

Copyright 2008 PCI Security Standards Council LLC

Programme d'assurance qualité

Le PCI SSC vérifie les rapports des PA-QSA dans une optique d'assurance qualité. Comme stipulé dans les *Exigences de conformité pour les évaluateurs de sécurité qualifiés* et dans l'*Accord PA-QSA*, les PA-QSA doivent respecter les critères d'assurance qualité définis par le PCI SSC. Les différentes étapes du programme d'assurance qualité sont décrites ci-dessous.

Le schéma du processus du programme d'assurance qualité est détaillé dans la Figure 5.

Programme d'échantillonnage pour les nouveaux QSA

Le PCI SSC applique une procédure d'échantillonnage évolutive pour vérifier les Rapports sur la conformité élaborés par les PA-QSA – au début, le PCI SSC vérifie beaucoup de rapports, puis le taux d'échantillonnage réduit à mesure que les rapports des PA-QSA gagnent en qualité. Si le PA-QSA maintient le niveau de qualité, il passe au programme d'échantillonnage pour les QSA expérimentés (avec des taux d'échantillonnage plus faibles). Tant que le PA-QSA maintient le niveau de qualité, il est soumis à un échantillonnage limité.

Dans le cas contraire, les mesures suivantes sont appliquées :

- Lettre d'avertissement : envoyée au PA-QSA en guise de premier rappel l'incitant à améliorer la qualité de ses rapports ;
- Rattrapage : Si le niveau de qualité n'est pas maintenu, le PA-QSA passe en phase de rattrapage et peut se voir infliger des sanctions.
- Révocation : Si le niveau de qualité n'est pas maintenu, le PA-QSA est révoqué et retiré de la liste des PA-QSA agréés du PCI SSC.

Programme d'échantillonnage pour les PA-QSA expérimentés

Une fois le PA-QSA soumis au programme d'échantillonnage pour les PA-QSA expérimentés, un échantillonnage limité est appliqué à ses rapports. Si le niveau de qualité est maintenu, l'échantillonnage limité se poursuit. Cette procédure a pour but de maintenir les PA-QSA dans un « état stable ».

Si des problèmes de qualité sont détectés et si le niveau de qualité n'est pas maintenu, le PA-QSA repasse au programme d'échantillonnage pour les nouveaux QSA.

Rattrapage

En phase de rattrapage, les PA-QSA peuvent toujours réaliser des vérifications, mais tous les rapports sont vérifiés par le PCI SSC dans une optique d'assurance qualité. Le PCI SSC facturera 500 $ pour chaque rapport soumis et resoumis en phase de rattrapage.

Le PA-QSA doit également soumettre un plan de rattrapage au PCI SSC précisant comment il prévoit d'améliorer la qualité de ses rapports. Le PCI SSC peut également exiger une visite sur site avec le PA-QSA pour auditer son programme d'assurance qualité, et ce à la charge du PA-QSA.

Si le PA-QSA atteint un niveau de qualité satisfaisant en phase de rattrapage, il est de nouveau soumis au programme d'échantillonnage pour les nouveaux PA-QSA. S'il n'y parvient pas, il passe à la phase de Révocation.

Notez que si une application de paiement figurant dans la liste du PCI SSC des applications de paiement conformes à la norme PA-DSS est compromise par une erreur émanant du PA-QSA, celui-ci passe immédiatement en phase de rattrapage. Le PA-QSA doit atteindre un niveau de qualité satisfaisant pour être de nouveau soumis au programme d'échantillonnage pour les nouveaux PA-QSA.

Copyright 2008 PCI Security Standards Council LLC

Révocation

Lorsqu'un PA-QSA est révoqué, il est retiré de la liste des PA-QSA agréés du PCI SSC. Dès lors, il ne peut plus réaliser de vérifications d'applications de paiement. Il peut faire appel contre sa mise en révocation, mais doit respecter les exigences, conformément aux exigences de conformité pour les évaluateurs de sécurité qualifiés et aux documents annexes. Le PCI SSC se réserve le droit d'exiger un examen blanc.

Avant d'être de nouveau soumis au programme d'échantillonnage pour les nouveaux PA-QSA, les PA-QSA doivent régler des frais de réinscription sur la liste s'élevant à 1 250 $.

Copyright 2008 PCI Security Standards Council LLC

Processus d'acceptation des rapports PA-DSS

Le PCI SSC base l'acceptation des rapports uniquement sur les résultats documentés figurant dans le Rapport sur la conformité. À la réception du rapport, les scénarios suivants peuvent se dérouler :

- Le PCI SSC vérifie le rapport (généralement dans les trente jours civils suivant la réception) et détermine s'il est acceptable ou non.
- Si aucun problème (ou aucune question) à communiquer au PA-QSA n'est soulevé(e), le PCI SSC adresse au fournisseur de logiciels la facture relative aux frais d'inscription. Une fois le règlement des frais d'inscription reçu, le PCI SSC émet une lettre d'acceptation PA-DSS et publie l'application de paiement et les informations concernant le fournisseur sur le site Web.
- Si des questions ou des problèmes sont soulevés et communiqués au PA-QSA, la procédure décrite ci-dessus reprend à compter de la réception d'un rapport (ou d'une réponse) complet, acceptable et révisé (« Rapport révisé ») fourni par le PA-QSA. La procédure ne redémarre qu'à la réception d'un rapport révisé acceptable traitant tous les éléments précédemment identifiés mais restant en instance. Généralement, le PCI SSC vérifie les rapports révisés dans les quatorze jours civils suivant leur réception.
- Si d'autres questions ou problèmes apparaissent, le cycle se répète jusqu'à réception d'une réponse satisfaisante. Ce n'est qu'à ce moment-là que le PCI SSC émet la lettre d'acceptation PA-DSS et publie les informations appropriées sur le site Web. Il est possible de soulever des questions ou des problèmes supplémentaires à tout moment avant l'émission de la lettre d'acceptation PA-DSS.

Pour les rapports relatifs aux modifications apportées aux versions des applications répertoriées existantes, basés sur l'auto-attestation de modification des fournisseurs, le processus d'acceptation des rapports PA-DSS est identique à celui indiqué ci-dessus ; le PCI SSC doit émettre une lettre d'acceptation PA-DSS révisée et publier les informations mises à jour sur le site Web, à moins que des questions soient soulevées, d'une façon similaire à celle mentionnée ci-dessus.

La lettre d'acceptation du PCI SSC et l'inscription sur le site Web doivent contenir au minimum les informations ci-dessous. Chaque caractéristique est détaillée dans l'*annexe A : Éléments de la lettre d'acceptation et de la liste des applications de paiement conformes à la norme PA-DSS.*

- Fournisseur de l'application de paiement
- Identifiant de l'application de paiement
- Numéro d'approbation
- Notes de conformité
- Notes de déploiement
- Auto-attestation pour les modifications mineures de versions, le cas échéant
- Date de revalidation annuelle
- Date d'expiration
- Société PA-QSA
- Type d'application de paiement
- Marché visé par l'application de paiement, le cas échéant
- Région ou localité spécifique pour l'application de paiement, le cas échéant

***Remarque** :*

Le PCI SSC ne garantit aucune « approbation partielle » par rapport à la capacité d'une application de paiement à respecter certaines exigences, et non la totalité d'entre elles.

Copyright 2008 PCI Security Standards Council LLC

Notification faisant suite à une faille ou à un incident de sécurité

Les fournisseurs se doivent d'informer le PCI SSC de toute faille ou de tout incident de sécurité en rapport avec une application de paiement répertoriée, en appliquant les procédures décrites dans cette section.

Notification et gestion du temps

Nonobstant toute autre obligation légale s'appliquant au fournisseur, celui-ci doit immédiatement informer le PCI SSC de toute faille ou de tout incident de sécurité en rapport avec l'une de ses applications de paiement répertoriées par le PCI SSC.

De la même façon, le fournisseur doit donner immédiatement un retour sur l'impact potentiel (possible ou actuel) que la faille a entraîné, peut ou pourra entraîner.

Remarque :

La notification doit avoir lieu moins de 24 heures après la découverte par le fournisseur de la faille ou de l'incident de sécurité.

Format de notification

La première notification d'une faille ou d'un incident de sécurité élaborée par le fournisseur doit prendre la forme d'un appel téléphonique au coordinateur PCI SSC PA-DSS, suivi d'un message électronique, d'une télécopie ou d'une lettre détaillant la faille ou l'incident de sécurité.

Détails de la notification

Suite à la notification d'une faille ou d'un incident de sécurité, le fournisseur doit transmettre au coordinateur PCI SSC PA-DSS toutes les informations pertinentes relatives à cette faille ou à cet incident de sécurité. Cela peut inclure, mais sans s'y limiter, les éléments suivants :

- le nombre de comptes compromis (s'il est connu) ;
- tous les rapports détaillant la faille ou l'incident de sécurité ;
- l'ensemble des rapports ou évaluations réalisés à des fins d'investigation sur la faille ou l'incident de sécurité.

Le PCI SSC, conformément aux termes de l'accord de diffusion, a la possibilité de partager ces informations et les autres informations requises pour prendre en charge ou autoriser l'exécution d'une évaluation de la faille ou de l'incident de sécurité afin d'atténuer les risques ou d'empêcher tout nouvel incident du même type.

Actions faisant suite à une faille ou à un incident de sécurité

Si le PCI SSC détecte une faille au niveau de la sécurité ou un incident relatif à un produit spécifique ou à un groupe de produits, comme ceux répertoriés dans la liste des applications de paiement conformes à la norme PA-DSS, il peut appliquer les mesures suivantes :

- Informer toutes les marques de cartes de paiement qu'une faille ou un incident de sécurité s'est produit.
- Tenter d'obtenir le rapport officiel pour évaluer avec précision la façon dont l'incident s'est produit.
- Contacter le fournisseur pour lui signaler qu'une faille de sécurité a été détectée sur son produit, ou que celui-ci a été compromis et, si possible, partager les informations relatives à la faille ou l'incident en question.
- Poursuivre les efforts entrepris par le fournisseur pour tenter d'atténuer les risques ou d'empêcher tout nouvel incident du même type.

Copyright 2008 PCI Security Standards Council LLC

- Poursuivre les efforts entrepris par le fournisseur pour 1) corriger les failles de sécurité et 2) rédiger un document regroupant les directives à transmettre aux clients de ce fournisseur, document les informant sur les vulnérabilités potentielles et détaillant les actions à entreprendre pour atténuer les risques ou empêcher tout nouvel incident du même type.
- Travailler avec des organismes d'application des lois afin d'atténuer les risques ou d'empêcher tout nouvel incident du même type.
- Prendre en charge et/ou autoriser les évaluations sur le produit compromis en interne ou selon les termes de l'accord de diffusion en faisant appel aux PA-QSA pour identifier l'origine de l'incident.

Retrait d'approbation

Le PCI SSC se réserve le droit de retirer l'acceptation d'une application de paiement et de la supprimer de la *liste des applications de paiement conformes à la norme PA-DSS*, lorsqu'il est clair que l'application de paiement ne dispose pas d'une protection suffisante contre les menaces actuelles et/ou n'est pas conforme aux exigences PA-DSS. Si le PCI SSC considère que l'application de paiement a une faille de sécurité ou a été compromise, il informe le fournisseur par écrit qu'il a l'intention de retirer son acceptation concernant cette application de paiement.

Copyright 2008 PCI Security Standards Council LLC

Clauses et conditions légales

L'approbation du PCI SSC s'applique uniquement aux applications de paiement/versions identiques à l'application de paiement vérifiée par un PA-QSA. Si un aspect de l'application de paiement diffère de celle qui a été testée par le PA-QSA, même si l'application de paiement est conforme à la description de base du produit figurant dans la lettre, l'application de paiement ne doit pas être considérée comme acceptée par le PCI SSC, ni obtenir le statut « Acceptée ». Par exemple, si une application de paiement porte le même nom ou le même numéro de version qu'une application de paiement vérifiée par le PA-QSA, alors qu'elle n'est pas identique à cette dernière, elle ne doit pas être considérée comme acceptée ou obtenir le statut « Acceptée ».

Aucun fournisseur ni partie tierce ne peut se référer à une application de paiement ayant le statut « Approuvée par la PCI » ou « Approuvée par le PCI SSC », ni en aucun cas déclarer ou laisser supposer que le PCI SSC a, intégralement ou partiellement, approuvé un aspect de l'activité d'un fournisseur ou de ses applications de paiement, sauf dans la mesure et selon les termes et restrictions expressément définis dans un accord écrit avec le PCI SSC ou dans une lettre d'acceptation PA-DSS. Toutes les autres références à l'acceptation du PCI SSC sont strictement interdites par le PCI SSC.

Le PCI SSC accorde une acceptation pour garantir certains critères de sécurité et de mise en œuvre qui lui permettent d'atteindre ses objectifs. Toutefois, cette acceptation ne doit en aucun cas inclure d'approbation ou de garantie sous quelque forme que ce soit par rapport à la fonctionnalité, à la qualité ou aux performances d'un produit ou d'un service particulier. Le PCI SSC ne garantit aucun produit ou service fourni par des tierces parties. L'acceptation n'inclut ou n'implique en aucun cas de garanties de produits émanant du PCI SSC, y compris, mais sans s'y limiter, toute garantie implicite de qualité loyale et marchande et d'adéquation à une activité spécifique ou de non-violation, ces garanties étant toutes expressément déclinées par le PCI SSC. L'ensemble des droits et des recours concernant les produits et les services ayant obtenu une acceptation doivent émaner de la partie fournissant les produits et services en question, et non par le PCI SSC ou les marques de cartes de paiement.

Sauf stipulation contraire indiquée par écrit par le PCI SSC, l'ensemble des biens et services spécifiés dans ce document, que le PCI SSC a transmis aux parties tierces concernées, sont fournis « en l'état » et « avec tous les défauts », sans garantie de quelque nature que ce soit.

Copyright 2008 PCI Security Standards Council LLC

Annexe A : Éléments de la lettre d'acceptation et de la *liste des applications de paiement conformes à la norme PA-DSS*

Fournisseur de l'application de paiement

Ce champ désigne le **fournisseur de l'application de paiement** à valider.

Identifiant de l'application de paiement

L'**identifiant de l'application de paiement** indique au PCI SSC les informations relatives à une application de paiement validée. Il comprend les éléments suivants :

- nom de l'application de paiement ;
- numéro de version de l'application de paiement.

Afin de garantir l'utilisation d'une application de paiement validée, il est fortement recommandé aux clients acquéreurs ou à leurs agents désignés d'acheter et de déployer uniquement les applications de paiement dont les informations associées correspondent exactement à celles de l'identifiant de l'application de paiement. Exemple d'**identifiant d'application de paiement** (deux composants) :

Composant	Description
Nom de l'application	Acme Payment 600
Numéro de version de l'application	PCI 4.53

Numéro de version de l'application

Le **numéro de version de l'application** correspond au numéro de l'application spécifique vérifiée lors de l'évaluation PA-DSS. Il peut être constitué d'un ensemble de caractères alphanumériques fixes ou variables.

Remarque :

Pour plus d'informations sur le contenu à inclure dans le Rapport sur la conformité PA-DSS concernant les méthodologies de gestion des versions appliquées par le fournisseur, reportez-vous à la section Instructions et contenu du Rapport sur la conformité.

Il est fortement recommandé aux clients d'acheter et de déployer uniquement des applications portant le numéro de version d'application comprenant exactement les mêmes caractères alphanumériques que celui de l'application figurant sur la liste des applications de paiement conformes à la norme PA-DSS ou sur la lettre d'acceptation PA-DSS émise par le PCI SSC.

Numéro d'approbation

Le PCI SSC attribue un **numéro d'approbation** au moment de l'acceptation. Ce numéro reste le même tant que l'application figure sur la liste.

Notes de conformité

Les **notes de conformité** permettent au PCI SSC de déterminer si la vérification a été réalisée en fonction du programme PABP de Visa ou du programme PA-DSS du PCI SSC. Elles permettent également de connaître la version applicable du programme PABP ou de la norme PA-DSS. Reportez-vous aux exemples du tableau dans la section Notes de déploiement ci-dessous.

Copyright 2008 PCI Security Standards Council LLC

Notes de déploiement

Les **notes de déploiement** permettent au PCI SSC de déterminer si une application de paiement est acceptable ou non pour les nouveaux déploiements et si elle correspond à la date d'expiration appropriée, indiquée ci-dessous. Pour plus d'informations, reportez-vous au tableau page 25.

Liste du PCI SSC avant expiration		Liste du PCI SSC après expiration	
Notes de conformité	**Notes de déploiement**	**Notes de conformité**	**Notes de déploiement**
Conforme au programme PABP	Acceptable pour les nouveaux déploiements	Conforme au programme PABP	Inacceptable pour les nouveaux déploiements
Application pré-PCI	Déconseillé pour les nouveaux déploiements	Application pré-PCI	Inacceptable pour les nouveaux déploiements
Conforme à la norme PA-DSS	Acceptable pour les nouveaux déploiements	Conforme à la norme PA-DSS	Inacceptable pour les nouveaux déploiements

Auto-attestation pour les modifications mineures de versions, le cas échéant

L'**auto-attestation pour les modifications mineures de versions** permet de spécifier, le cas échéant, les versions d'applications auxquelles s'applique la procédure pour les modifications mineures apportées aux applications, documentée dans la section *Aucun impact sur les exigences PA-DSS* de ce document.

Date de revalidation annuelle

La **date de revalidation annuelle** permet au PCI SSC de savoir quand l'attestation de conformité annuelle du fournisseur de logiciels arrive à échéance. Une section sur la revalidation annuelle figure dans le formulaire d'attestation de conformité, qui se trouve dans la partie 3b de l'annexe C de la norme PA-DSS.

Date d'expiration

La **date d'expiration** des applications de paiement conformes à la norme PA-DSS correspond à la date à laquelle un fournisseur doit faire réévaluer son application, conformément aux exigences de la norme PA-DSS en vigueur, afin de conserver son acceptation. La date d'expiration se rapporte aux notes de déploiement susmentionnées.

Le PCI SSC s'efforcera de mettre à jour la norme PA-DSS sur une base de 24 mois, conjointement aux mises à jour des normes PCI DSS. L'acceptation des applications de paiement conformes à la norme PA-DSS expire trois ans après la date effective d'une mise à jour des exigences PA-DSS. L'objectif est fixé à un minimum de trois ans d'approbation, sous réserve de menaces susceptibles de nécessiter des modifications immédiates.

Remarque :

Toute évaluation PA-DSS réalisée par rapport à la norme PA-DSS version 1.1 obtient la même date d'expiration que les vérifications effectuées par rapport à la version 1.2, conformément à la procédure normale d'expiration.

Exemple : Les versions 1.1 et 1.2 de la norme PA-DSS expireront à la même date. Avec la version suivante de la norme PA-DSS (faisant suite à la version 1.2), dont la sortie est prévue en octobre 2010, les vérifications par rapport aux versions 1.1 et 1.2 expireront en octobre 2013.

Actuellement, les applications de paiement conformes à la norme PA-DSS figurant sur la liste agréée au moment de leur déploiement n'ont pas de date d'expiration. Les applications de paiement déployées dont les approbations ont expiré peuvent encore être utilisées. Le calendrier d'expiration s'applique aux nouveaux achats/déploiements, et non aux déploiements existants.

Copyright 2008 PCI Security Standards Council LLC

Société PA-QSA

Ce champ indique le nom de la **société d'évaluateurs de sécurité qualifiés des applications de paiement** qui ont réalisé la vérification et déterminé si l'application de paiement était conforme à la norme PA-DSS.

Type d'application de paiement

Le **type d'application de paiement** désigne l'un des éléments suivants :

- Point de vente
- Middleware (intergiciel)
- Pompe à essence automatisée
- Panier d'achat
- Règlement
- Carte absente
- Passerelle
- Autre

Marché visé

Le **marché visé** correspond au marché cible de l'application de paiement, le cas échéant. Les marchés suivants constituent des exemples de marchés visés :

- Vente au détail
- Kiosques pour les parcs de stationnement
- Essence/huile
- Commerce électronique

Remarque :

Ces éléments permettent de déterminer si l'application de paiement est conçue pour un marché particulier, et non à des seules fins de marketing pour le fournisseur de logiciels.

Région ou localité spécifique pour l'application de paiement, le cas échéant

La région ou localité spécifique pour l'application de paiement s'applique aux applications de paiement qui sont exclusivement développées pour des régions ou localités géographiques spécifiques.

Copyright 2008 PCI Security Standards Council LLC

Annexe B : Identification des builds d'applications de paiement certifiées

Remarque : *À l'étude*.

Même si les builds d'applications de paiement certifiées ne constituent pas aujourd'hui une exigence, nous encourageons les fournisseurs de logiciels et les PA-QSA à travailler de concert pour développer des méthodes permettant de certifier et d'approuver les builds d'applications de paiement de façon numérique. Le PCI SSC se réserve le droit d'exiger, à l'avenir, les builds d'applications de paiement certifiées.

Une telle méthode pourrait par exemple inclure les éléments suivants :

Les fournisseurs identifient clairement une build certifiée à des fins de publication. Dans l'idéal, une build certifiée conforme par un PA-QSA doit contenir l'empreinte numérique (codée) du fournisseur de logiciels et celle du QSA, apposée au moment de l'expédition. Au minimum, la livraison doit être clairement identifiée par le nom, la version, le numéro de build et l'horodatage, et doit pouvoir être vérifiée par un prétraitement MD5 et par l'en-tête de build correspondante. De cette façon, l'exigence 7.2 de la norme PA-DSS concernant la garantie d'expédition via la « chaîne de confiance connue » est renforcée. Cette méthode permettrait également de prendre en charge les programmes PA-DSS relatifs aux marques de cartes de paiement, et d'encourager la sensibilisation et la confiance des clients.

Copyright 2008 PCI Security Standards Council LLC

Annexe C : Auto-attestation pour les modifications mineures de versions

Instructions de transmission

Le fournisseur de l'application de paiement et l'évaluateur de sécurité qualifié des applications de paiement (PA-QSA) doivent remplir ce document qui fait office de déclaration sur l'état de conformité de l'application de paiement vis-à-vis de la norme de sécurité des données des applications de paiement (PA-DSS). Le fournisseur de l'application de paiement doit remplir toutes les sections et transmettre au PA-QSA le document d'analyse de changement accompagné de la présente auto-attestation.

Suite à la vérification de la documentation fournie, le PA-QSA doit remplir les sections applicables et transmettre ce document au PCI SSC, accompagné des copies de tous les documents requis, en respectant les instructions du PCI SSC en matière de cryptage et de transmission des rapports.

Partie 1. Informations sur le fournisseur de l'application de paiement					
Nom de l'entreprise :					
Nom du contact :		Poste occupé :			
Téléphone :		Adresse électronique :			
Adresse professionnelle :		Ville :			
État/province :		Pays :		Code postal :	
URL :					

Partie 1a. Informations sur l'application de paiement	
Nom et numéro de version de l'application de paiement « parente » figurant actuellement sur la liste du PCI SSC :	
Nom de l'application existant :	Numéro de version existant :
Numéro d'approbation du PCI SSC :	
Nouveaux nom et numéro de version de l'application de paiement, le cas échéant :	
Nouveau nom de l'application :	Nouveau numéro de version :
Description des modifications, le cas échéant :	

Fonctionnalités de l'application de paiement (cocher toutes les cases correspondantes) :

☐ Point de vente	☐ Panier d'achat	☐ Carte absente
☐ Middleware (intergiciel)	☐ Règlement	☐ Passerelle :
☐ Pompe à essence automatisée	☐ Autres (préciser) :	

Copyright 2008 PCI Security Standards Council LLC

Marché visé par l'application :

Copyright 2008 PCI Security Standards Council LLC

Partie 2. Informations sur la société PA-QSA

Nom de l'entreprise :					
Nom du principal contact PA-QSA :		Poste occupé :			
Téléphone :		Adresse électronique :			
Adresse professionnelle :		Ville :			
État/province :		Pays :		Code postal :	
URL :					

Partie 3. Confirmation du statut de modification

Partie 3a. Attestation du fournisseur de l'application de paiement

En se basant sur l'analyse de changement interne et sur la documentation de l'analyse de changement, *(PA Vendor Name)* déclare le statut suivant pour la ou les applications et versions identifiées dans la partie 1a de ce document au *(date)* (cocher les cases correspondantes) :

☐	*Des modifications mineures uniquement* ont été apportées à l'application « parente » indiquée ci-dessus, dans le but de créer la nouvelle application également susmentionnée n'impliquant **aucun impact** sur les exigences PA-DSS.
☐	Toutes les modifications ont été inscrites avec exactitude dans le document d'analyse de changement de la partie 2 transmis au PA-QSA.
☐	Toutes les informations figurant dans cette auto-attestation illustrent en toute honnêteté les résultats de l'analyse de changement, à tous points de vue.
☐	Il n'existe aucune preuve de stockage de données de bande magnétique (c'est-à-dire de pistes)[4], de données CAV2, CVC2, CID ou CVV2[5] ou de données PIN[6] suite à l'autorisation d'une transaction sur TOUT fichier ou fonctionnalité généré(e) par l'application.

Partie 3b. Attestation du PA-QSA

En se basant sur la documentation d'analyse de changement délivrée par le fournisseur de l'application de paiement indiqué dans la partie 1, *(PA-QSA Name)* déclare le statut suivant pour la ou les applications et versions identifiées dans la partie 1a de ce document au *(date)* (cocher les cases correspondantes) :

☐	En se basant sur notre vérification de la documentation de l'analyse de changement, nous attestons que la documentation prend en charge l'affirmation du fournisseur selon laquelle *des modifications mineures uniquement* ont été apportées à l'application susmentionnée, n'impliquant ainsi **aucun impact** sur les exigences PA-DSS.

[4] Données de bande magnétique (piste) : Données encodées sur la bande magnétique utilisée pour une autorisation lors d'une transaction carte présente. Les entités ne peuvent pas conserver l'ensemble des données sur bande magnétique après autorisation. Les seuls éléments de données de piste pouvant être conservés sont le numéro de compte, la date d'expiration et le nom du détenteur.

[5] La valeur à trois ou quatre chiffres imprimée sur l'espace dédié à la signature ou sur la face avant d'une carte de paiement, utilisée pour vérifier les transactions carte absente.

[6] Les données PIN (Personal Identification Number, numéro d'identification personnel) désignent le code saisi par le titulaire de la carte lors d'une transaction carte présente, et/ou le bloc PIN crypté présent dans le message de la transaction.

Copyright 2008 PCI Security Standards Council LLC

Partie 3c. Ratification par le PA-QSA et le fournisseur de l'application

Signature du PA-QSA principal ↑	*Date* ↑
Nom du PA-QSA principal ↑	*Poste occupé* ↑
Signature du cadre supérieur du fournisseur de l'application ↑	*Date* ↑
Nom du cadre supérieur du fournisseur de l'application ↑	*Poste occupé* ↑
Nom de l'entreprise fournissant l'application de paiement représentée ↑	

Copyright 2008 PCI Security Standards Council LLC